FIG. 1

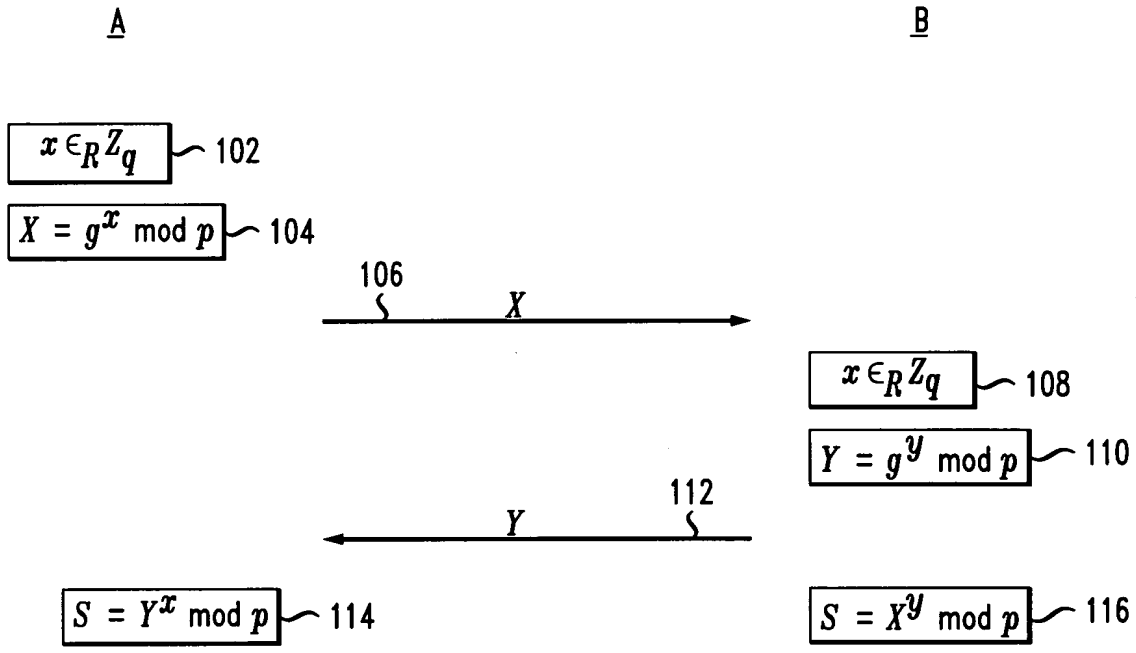

A
B
$x \in_R Z_q$
102
$X = g^x \bmod p$
104
106
X
$x \in_R Z_q$
108
$Y = g^y \bmod p$
110
112
Y
$S = Y^x \bmod p$
114
$S = X^y \bmod p$
116

FIG. 2

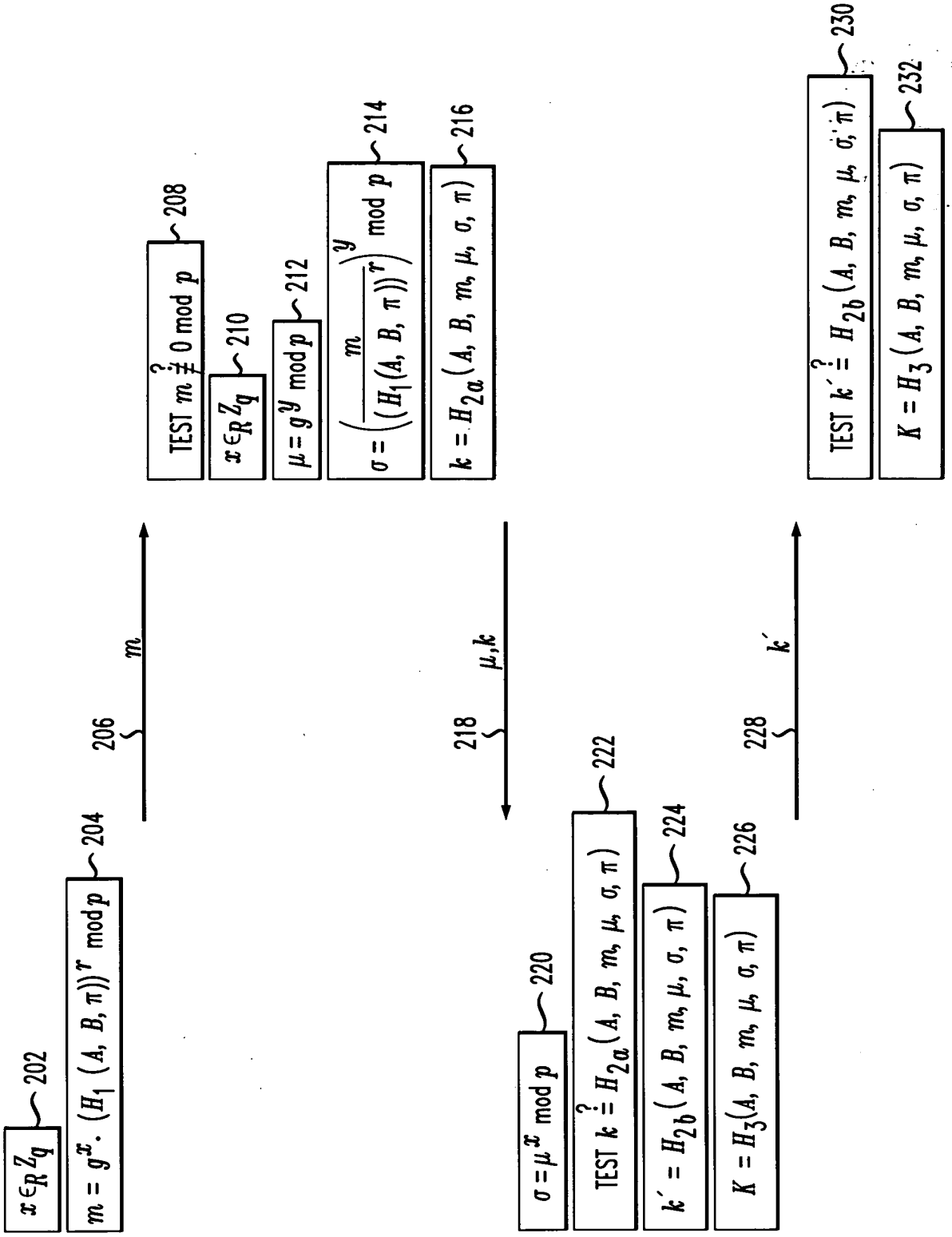

A
B
$x \in_R Z_q$ 202
$m = g^x \cdot (H_1(A, B, \pi))^r \bmod p$ 204
206 m
TEST $m \stackrel{?}{\neq} 0 \bmod p$ 208
$x \in_R Z_q$ 210
$\mu = g^y \bmod p$ 212
$\sigma = \left(\frac{m}{(H_1(A, B, \pi))^r}\right)^y \bmod p$ 214
$k = H_{2a}(A, B, m, \mu, \sigma, \pi)$ 216
218 μ,k
$\sigma = \mu^x \bmod p$ 220
TEST $k \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi)$ 222
$k' = H_{2b}(A, B, m, \mu, \sigma, \pi)$ 224
$K = H_3(A, B, m, \mu, \sigma, \pi)$ 226
228 k'
TEST $k' \stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi)$ 230
$K = H_3(A, B, m, \mu, \sigma, \pi)$ 232

FIG. 3

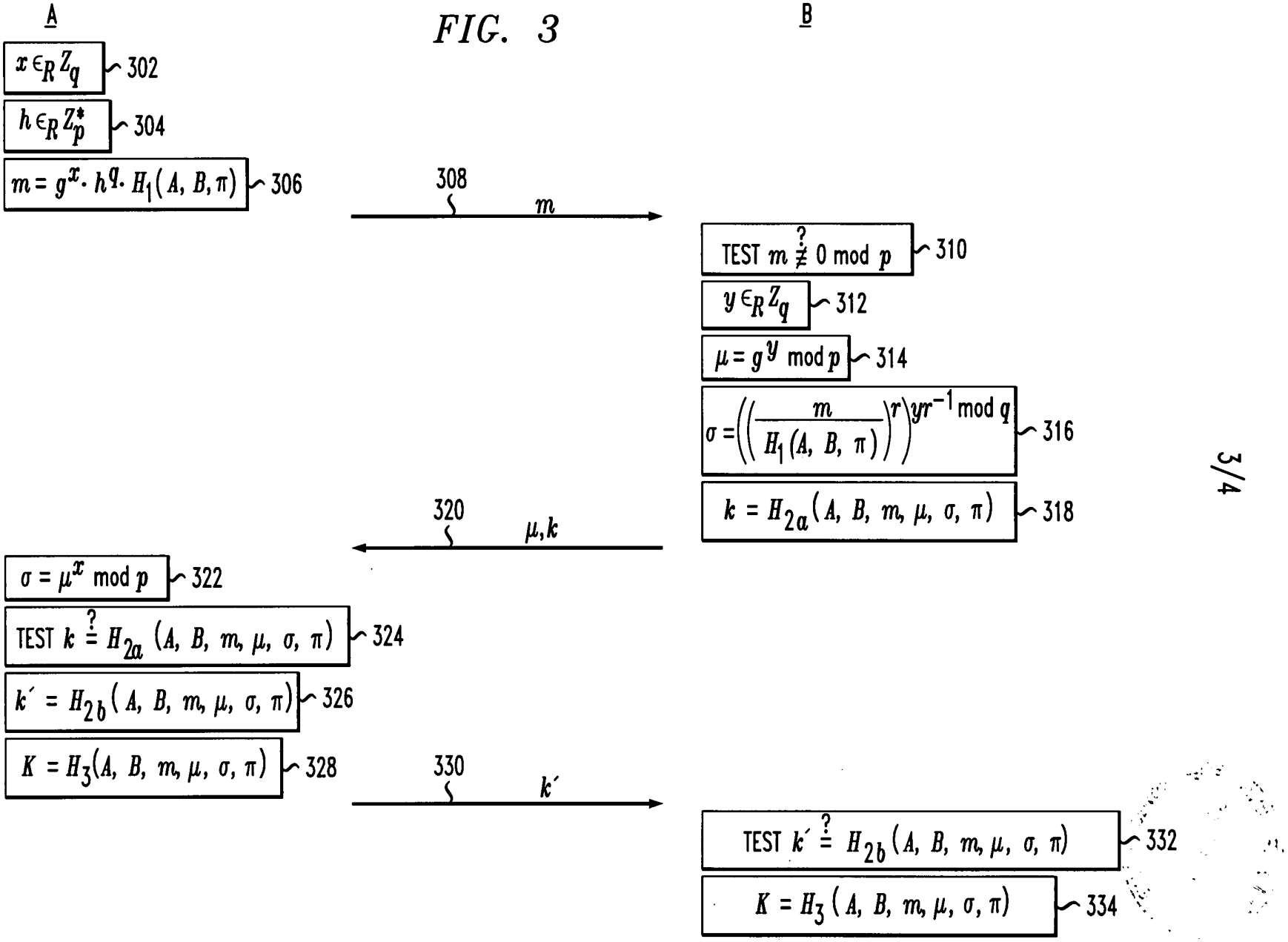
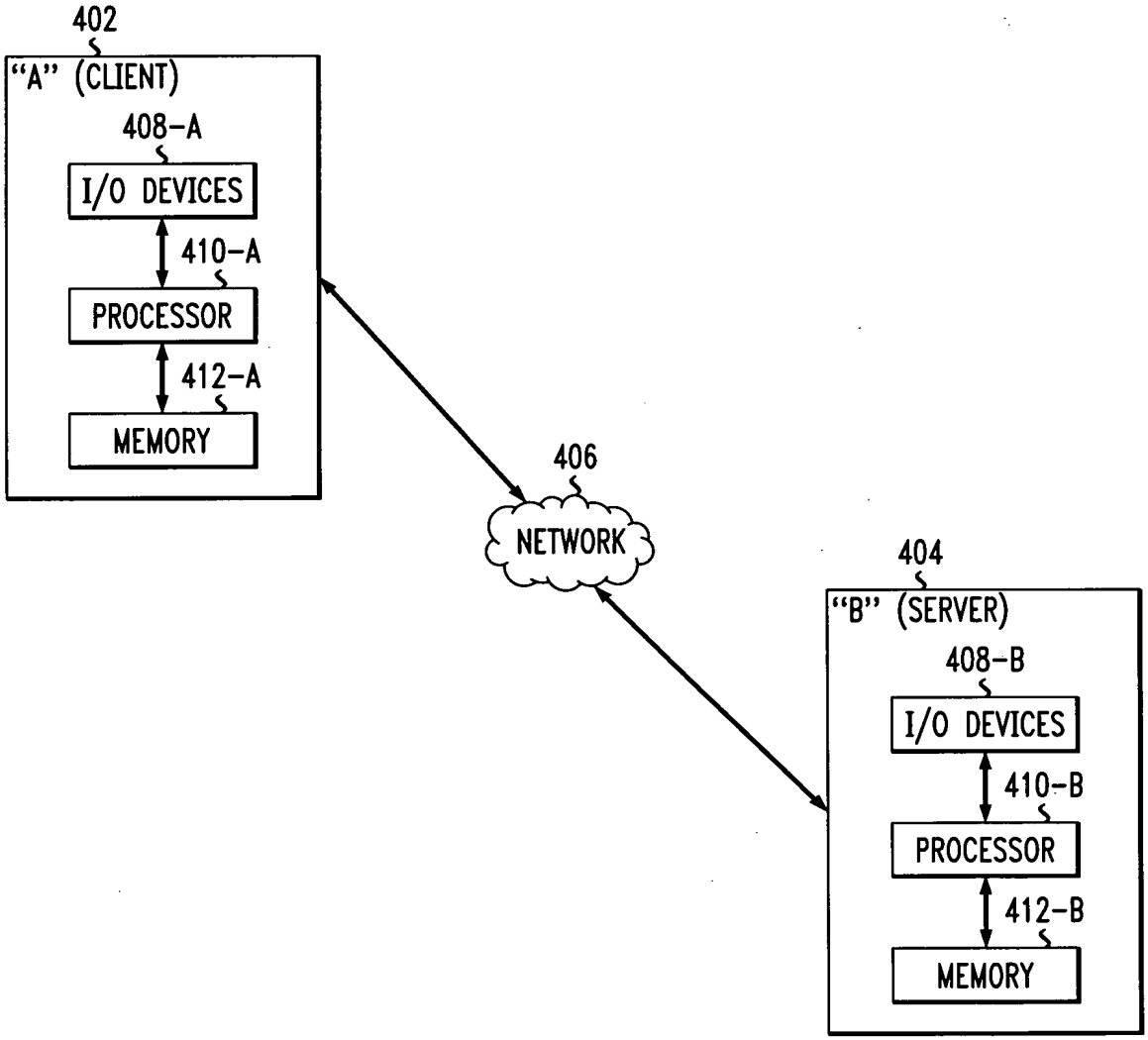

A
B
$x \in_R Z_q$ 302
$h \in_R Z_p^*$ 304
$m = g^x \cdot h^q \cdot H_1(A, B, \pi)$ 306
308
m
TEST $m \stackrel{?}{\neq} 0 \bmod p$ 310
$y \in_R Z_q$ 312
$\mu = g^y \bmod p$ 314
$\sigma = \left(\left(\frac{m}{H_1(A, B, \pi)}\right)^r\right)^{yr^{-1}} \bmod q$ 316
$k = H_{2a}(A, B, m, \mu, \sigma, \pi)$ 318
320
μ, k
$\sigma = \mu^x \bmod p$ 322
TEST $k \stackrel{?}{=} H_{2a}(A, B, m, \mu, \sigma, \pi)$ 324
$k' = H_{2b}(A, B, m, \mu, \sigma, \pi)$ 326
$K = H_3(A, B, m, \mu, \sigma, \pi)$ 328
330
k'
TEST $k' \stackrel{?}{=} H_{2b}(A, B, m, \mu, \sigma, \pi)$ 332
$K = H_3(A, B, m, \mu, \sigma, \pi)$ 334

FIG. 4


402
"A" (CLIENT)
408-A
I/O DEVICES
410-A
PROCESSOR
412-A
MEMORY
406
NETWORK
404
"B" (SERVER)
408-B
I/O DEVICES
410-B
PROCESSOR
412-B
MEMORY